Incident Management Process Flowchart (V2)

This document details the improved incident management process, ensuring efficient resolution of reported issues. The workflow includes structured triage, automated resolution pathways, impact classification, and follow-up mechanisms to enhance response efficiency and escalation handling.

Step-by-Step Process:

- Start

The incident management process begins. This signifies the point where an issue is reported or detected, triggering the workflow.

- User Reports Issue

A user experiences a problem and submits an incident report. This can be done through various channels, such as a ticketing system, email, or direct call to the support team. The details provided by the user, including error messages, timestamps, and impact assessments, are crucial for efficient resolution.

- Initial Triage

The support team performs an initial assessment of the incident to determine its urgency, scope, and potential resolution path. This step helps filter simple issues from complex ones, ensuring that resources are allocated appropriately.

- Classify Incident

The incident is categorized based on its nature (e.g., hardware failure, software bug, network issue). Proper classification ensures that the correct resolution protocol is followed and that the appropriate team is assigned.

- Automated Resolution?

A decision is made regarding whether the issue can be resolved automatically. Some common automated solutions include system reboots, automated scripts for patching, or self-healing mechanisms. If automation is possible, the process moves directly to closing the ticket.

- High Impact?

The impact of the incident is assessed. If the issue affects critical business functions, large user groups, or essential services, it is classified as 'High Impact,' requiring priority handling.

- Critical?

For high-impact issues, an additional check determines whether the incident is critical. A 'Critical' classification is given if the issue threatens system security, data integrity, or core infrastructure. If critical, the incident is escalated immediately.

- Assign to Support Team

If the incident is neither critical nor resolvable via automation, it is assigned to the appropriate support team. The team members analyze logs, reproduce the issue if necessary, and start working on a resolution.

- Resolve Issue

The support team applies fixes, patches, or configuration changes to resolve the incident. This may involve collaboration with external vendors, development teams, or database administrators to implement a permanent solution.

- Issue Resolved?

A verification step is conducted to determine whether the applied fix has successfully resolved the problem. This includes user confirmation, system tests, and log analysis.

- Follow-up Needed?

If the issue is not fully resolved or requires monitoring, a follow-up process is initiated. This step ensures that similar incidents do not reoccur and that the fix is sustainable.

- Escalate to Higher Support

If the issue is unresolved or requires higher expertise, it is escalated to a senior technical team, specialized engineers, or external support. Escalation ensures that persistent or complex incidents receive additional scrutiny.

- Close Ticket

Once the issue is confirmed to be resolved and any necessary follow-ups are completed, the ticket is officially closed. Documentation of the incident and resolution steps is logged for future reference and knowledge base updates.